REMARKS

The Office Action of November 1, 2006, has been received and its contents carefully reviewed. By the above Amendment, Applicants have amended claims 1, 37, and 73-75 to more distinctly highlight the features of the present invention. Claims 1-75 remain pending in the application. No new matter is introduced by this Amendment. Thus, Applicants respectfully submit that the present application is in condition for allowance.

The rejection of claims 1-72 based on U.S. Patent No. 6,816,596 to *Peinado et al.* combined with U.S. Patent No. 6,697,948 to *Rabin et al.* is respectfully overcome, because *Peinado et al.* and *Rabin et al.*, taken alone or in combination, fail to disclose, teach or suggest all of the features recited in the pending claims. For example, independent claim 1, as amended (emphasis added), recites:

> A system for distributing digital documents having usage rights associated therewith, said system comprising:
> a server having at least one digital document stored thereon;
> a client computer having a standard application program including a rendering engine capable of being accessed to render content;
> a communications network coupled to said client and said server; and
> a security module which is downloaded and included in said client computer, the security module being adapted to be attached to the standard application program for enforcing security conditions for accessing the rendering engine,
> **wherein the security module intercepts requests to the rendering engine that would enact a violation of usage rights associated with the content and thus grants or denies the request to access the content based on the usage rights associated with the content.**

Independent claim 37, as amended (emphasis added), recites:

> A method for distributing digital documents having usage rights associated therewith, said method comprising:
> storing at least one digital document on a server;
> requesting, over a communications network, the at least one digital document from a client computer having a standard application program including a rendering engine capable of being accessed to render content; and
> enforcing security conditions for accessing the rendering engine with a security module which is downloaded and included in said client computer, the security module being adapted to be attached to the standard application program for enforcing security conditions,
> **wherein the security module intercepts requests to the rendering engine that would enact a violation of usage rights associated with the content and thus grants or denies the request to access the content based on the usage rights associated with the content.**

Thus, independent claims 1, and 37 include the novel features of a security module which is downloaded to and included in a client computer, the security module being adapted to be attached to the standard application program for enforcing security conditions, and wherein the security module intercepts requests to a rendering engine that would enact a violation of

usage rights associated with content and thus grants or denies the request to access the content based on the usage rights associated with the content.

By contrast, *Peinado et al.* fails to disclose, teach or suggest all of the features recited in independent claims 1 and 37. In addition, the combination of *Peinado et al.* and *Rabin et al.* would not be obvious to one of ordinary skill in the art, as *Rabin et al.* teaches away from necessitating the disclosure made in *Peinado et al.* Specifically, if one follows the teachings of *Rabin et al.*, there is no need to enforce or intercept access to the rendering engine of the protected content, because the rendering engine is trusted. In this respect, *Peinado et al.* discloses, at col. 34, lines 42-59, checks are made to verify the authenticity of the rendering engine, before the content is delivered to the rendering engine:

> As was set forth above, when the rendering application 34 sends digital content 12 to the black box 30 for decryption, the black box 30 and/or the DRM system 32 preferably authenticates that such rendering application 34 is in fact the same rendering application 34 that initially requested the DRM system 32 to run (step 531 of FIG. 5) and that the rendering application 34 itself satisfies any relevant terms in the corresponding digital license 16. In addition, such authentication ensures that such rendering application 34 can be trusted to handle the decrypted or 'naked' digital content 12 in an appropriate manner, and also that the rendering application 34 can be trusted to handle other sensitive matter (i.e., keys, encrypted matter, and/or other trusted matter). However, and referring now to FIG. 13, it is to be recognized that the digital content 12 likely will 'flow' in a path 58 from the rendering application 34 to an ultimate destination 60 by way of one or more modules 62 that define such path 58.

Thus, it is clear that *Peinado et al.* assumes that the rendering engine is trusted and will only perform actions on the content which would not violate usage rules of the content. As such, there is no need in *Peinado et al.*'s system to intercept access to the rendering engine by a separate trusted agent.

Nonetheless, even if there was motivation for combination, which is not the case, *Peinado et al.* and *Rabin et al.*, taken alone or in combination, still fail to disclose, teach or suggest all of the features recited in independent claims 1 and 37. Specifically, *Rabin et al.* discloses a system that precludes users from using software that is not licensed. The present Office Action highlights the following from *Rabin et al.*, col. 11, lines 9-34:

The step of receiving the instance of software can include the step of obtaining the instance of software at the user 10 device. And the step of receiving the tag at a user device can include the steps of securely obtaining the tag associated with the instance of software at the user device and determining if the tag associated with the instance of software is signed, and if so, verifying a signature on a hash function 15 value in the tag and if the signature on the hash function value is verified, installing the software on the user device, and if the tag associated with the instance of software is not signed, installing the instance of software on the user device. The step of detecting an attempt to use the instance of the 20 software on the user device can include the steps of invoking a supervising program on the user device to intercept a user request for use of the instance of software. The step of determining if the attempt to use the instance of the software is allowable can also include the steps of determining if a 25 call-up procedure is needed based on a call-up policy and if so performing a call-up procedure to verify the authenticity and to determine the usage supervision policy of the tag associated with the instance of software. Also included are the steps of updating tag information in the user device 30 based upon an outcome of the call-up procedure an examining status information associated with the tag to determine if use of the instance of software associated with the tag is allowed.

Thus, it is clear that the intent of *Rabin et al.* is to regulate *all access to the software*. By contrast, the invention of independent claims 1 and 37 would be directed to limiting access to such software, for example, only if/when it is operating on content that is protected. This type of selective intercept based on content, which is being processed, is not disclosed by *Peinado et al.* and *Rabin et al.*, taken alone or in combination.

In addition, while processing the protected content, if *Rabin et al.* where used to regulate access to the software, there is no conditional checking to regulate such access based on usage rules associated with such content. The regulation described by *Rabin et al.* is whether or not the user is authorized to use the software, not whether or not the requested action would violate the usage rules associated with the content.

Accordingly, in further response to the following assertions in the present Office Action:

enact a violation of usage rights associated with the content. However, within the same field of endeavor, Rabin teaches a system for protecting information, including a security module that intercepts requests to a rendering engine that would enact a violation of usage rights associated with the content [see Rabin, column 11, lines 9-34 and column 24, lines 33-48]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Rabin within the system of Peinado in order to further enhance security of the system.

Applicants submit that:

1)   It would not have been obvious to one of ordinary skill in the art to combine the teachings of *Rabin et al.* with *Peinado et al.*, as there is no need to do so. Specifically, *Peinado et al.* assumes that the rendering engine is trusted and verifies the authenticity of the rendering engine very clearly, and as such there is no need to employ the teachings of *Rabin et al.*

2)   Although *Rabin et al.* may disclose a system which regulates access to software generically without regard the type of content the software is processing, *Rabin et al.* does not disclose any type of regulation of access to the software based on what kind of content is being processed.

3)   *Rabin et al.* does not validate check or otherwise process "usage rules associated with the content."

4)   *Peinado et al.* fails to cure the noted deficiencies in *Rabin et al.*.

Accordingly, Applicants respectfully submit that independent claims 1 and 37 are allowable over *Peinado et al.* and *Rabin et al.*, alone or in combination. Dependent claims 2-36 and 38-75 are allowable over *Peinado et al.* on their own merits and for at least the reasons as argued above with respect to their independent claims.

Further, the present invention recited in independent claims 1, and 37 includes recognition of problems discovered with respect to conventional digital rights management (DRM) systems, for example, as described at page 2 of Applicants' Published Application:

> [0014] The second approach is to utilize proprietary formats wherein the document can only be rendered by a select rendering engine that is obligated to enforce the publisher's rights. Of course, this approach requires the use of a single proprietary format and loses the ability to combine plural popular formats and the richness of content associated therewith. Further, this approach requires the user to use a proprietary rendering application that must be obtained and installed on the user's computer and requires development of the rendering application for each format to be rendered in a secure manner. Further, the documents must be generated or converted using non-standard tools.

The present invention recited in independent claims 1, and 37, advantageously, addresses the discovered problems with respect to conventional DRM systems, for example, as described at page 6 of Applicants' Published Application:

[0063] The preferred embodiment utilizes a standard rendering engine of an application program, such as a browser, a word processor, or any other application or display program. The preferred embodiment achieves this by interfacing with the application and standing between the application and the document to control access to the document. Accordingly, a separate proprietary rendering engine for each document format is not required. Further, any data format supported by the application will be supposed by the invention without modification. It can be seen that the preferred embodiment permits DRM systems to be adapted to standards, such as TCP/IP and the use of browsers to render HTML. Further, the preferred embodiment facilitates various functionality that permits DRM to be applied to systems in a manner that is transparent to the user. Several examples of methods of operation of document distribution system 200 are described below.

By contrast, *Peinado et al.* and *Rabin et al.*, alone or in combination, fail to disclose, teach or suggest the noted features recited in independent claims 1, and 37, nor recognize or address the discovered problems with conventional DRM systems. Accordingly, one of ordinary skill in the art would find no motivation to arrive at the invention recited in independent claims 1, and 37, based on *Peinado et al.* and *Rabin et al.*, alone or in combination, absent improper hindsight reconstructions of Applicants' invention based on Applicants' disclosure.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. However, if the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

Respectfully submitted,

NIXON PEABODY, LLP

/Carlos R. Villamar, Reg. # 43,224/
Carlos R. Villamar
Reg. No. 43,224

NIXON PEABODY LLP
CUSTOMER NO.: 22204
401 9th Street, N.W., Suite 900
Washington, DC 20004
Tel: 202-585-8000
Fax: 202-585-8080

10552707.1